
SECURITY
Awareness

The Importance of Security Awareness Training

Security Awareness Training provides the knowledge to protect information systems and sensitive data from internal and external threats.

Online security awareness training is designed for how people learn and work today.

It is the responsibility of each employee to comply with agency policy and procedure in order to reduce security risks.

Information Security is not only concerned with threats coming from the outside of your agency.

Studies show that a company's biggest security threat is its own employees.

Are YOU the weakest link?

Physical Security
Why is it so important?

Physical security helps prevent loss, theft and unauthorized access.

- Lock up your computer and set a robust password to login.
- Secure laptop computers and mobile devices at all times.
- Don't leave mobile devices unattended in public locations.
- Don’t leave sensitive information lying around, including on printers, fax machines, or copiers.

Physical Security

- Shred media containing sensitive information when no longer using it …cd's, print outs, etc.
- Secure your area before leaving it unattended.
- Position your workstation so that unauthorized people and passers-by cannot see sensitive information on your monitor.
- Securely delete and erase all content of old computer, and mobile devices.

Controlled Area

An area in which uncontrolled movement will not result in compromise of confidential information.

Post a sign

Lock the door

Position away from viewing

Desktop Security

You have NO EXPECTATION OF PRIVACY

When you are away from your desk, either shut down or lock your terminal with password protection.

Set your computer to automatically lock when you are not using it.

FBI CJIS Security Policy states: "*The agency shall escort visitors at all times and monitor visitor activity. "*

Escort implies a physical and visual presence to the visitor at all times. Monitoring via security camera does not suffice as "escorting".

Visitor

As a best practice, it is recommended to maintain visitor access records (logs) to the physically secure location (except for those areas officially designated as publicly accessible) that includes:

- Name and agency of the visitor.
- Form of identification.
- Date of access.
- Time of entry and departure.
- Purpose of visit.
- Name and agency of person visited.

LONGER PASSWORDS

MAKE

STRONGER PASSWORDS

Password at a Minimum

- Be a **minimum** length of eight (8) characters.
- Not be a dictionary word or proper name.
- Not be the same as the User ID.
- Expire (change) at least every 90 days.
- Not be identical to the previous ten (10) passwords.
- Not be transmitted in the clear outside the secure location.
- Not be displayed when entered.

ID's and Passwords

Passwords are often a weak link in the authentication process.

Use phrases and misspelled words with embedded numbers and special characters.

Here are some WEAK passwords…do you know why??

Password - this is the most commonly used password and it is Pathetically weak…

Simple words can easily be guessed or broken with password hacker programs.

Marshall1963 - Though this uses 12 characters and includes letters and numbers…

Names that are associated with you or your family, or uses other identifying information such as birth year, are easily hacked.

Here are example passwords that discourage 'brute force' dictionary cracking:

Weak Password	**Better** Password	**Best** Password
Smellycat	Sm3llycat	Sm3llyc@t.
Julieloveskevin	JulieLovesKevin	Jul1eL0vesK3v1n
Ieatcarrots	IeatCarrots	I34carr0ts:
Ilovemypiano	ILoveMyPiano	ILov3MiPi@no
doctorhouse	DoctOrHOuse	.D0ct0H0use.

Can you see the difference???

More Password Tips…

- Add emoticons: Some websites limit the types of symbols you can use, most allow a wide range. ☺
- Don’t use the “Remember Password” feature of any application.
- Don’t use the same password on all sites.
- Use extra security for financial sites.

Don’t forget MOBILE DEVICES:

- Use a strong password/PIN to start up or resume activity, and automatically lock when not in use-- don't store anything you're not willing to lose.
- Some devices can be set to be erased remotely, or to erase themselves if the password/PIN is entered incorrectly a certain number of times.
- Consider turning these on to protect information in the case of theft or loss.

Information Handling

- Establish procedures for handling and storage of information to protect from unauthorized disclosure, alteration or misuse.

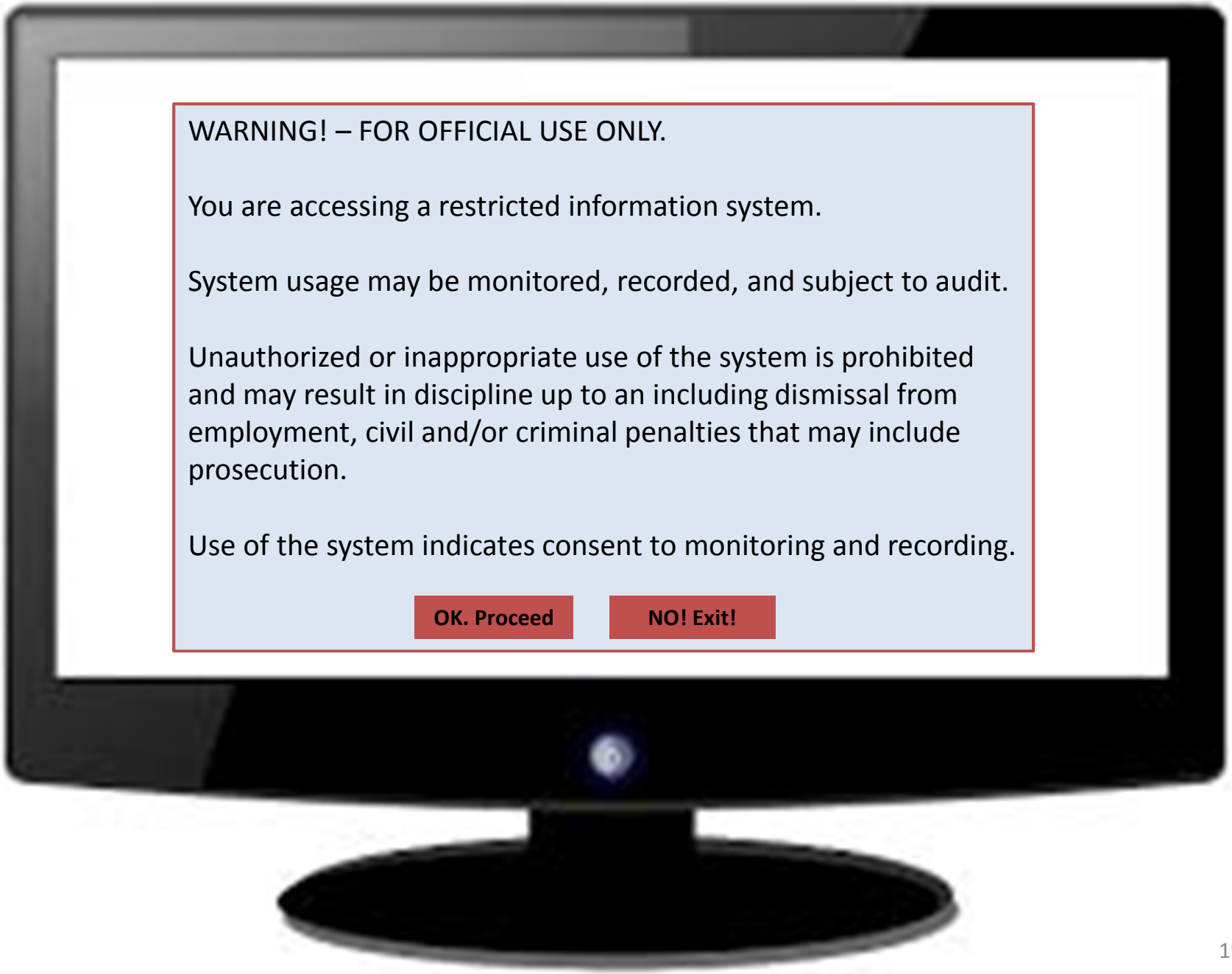
Standards of Discipline

Rea
net

The
to

Ent
cor
dis
cri

Suc



ay

Vulnerabilities and Threats

- A vulnerability is a point where a system is susceptible to attack.

  Vulnerabilities may include:

  - Physical
  - Natural
  - Media
  - Human
  - Communication
  - Hardware and Software

- While proper security measures such as anti-virus software can reduce the chance that an attack will succeed, NO information system is completely secure.

Threats

A threat is any potential danger to information or systems.

The threat is that someone, or something, will identify a specific vulnerability and use it against the agency or individual.

Threats can come from internal or external sources.

There are three main categories of threats:

- Natural
- Unintentional
- Intentional

Natural Threats

Natural Threats can endanger any facility or piece of equipment. You may not be able to prevent a natural disaster, but damage can be minimized with proper planning.

ARE YOU PREPARED?

Natural Threats

Natural threats include but are not limited to:

- Fire
- Flood
- Lightning
- Tornado
- Power Failures

Unintentional Threats

Unintentional threats are actions that occur due to lack of knowledge or through carelessness.

These threats can be prevented through awareness and training.

Unintentional Threats:

These may include:

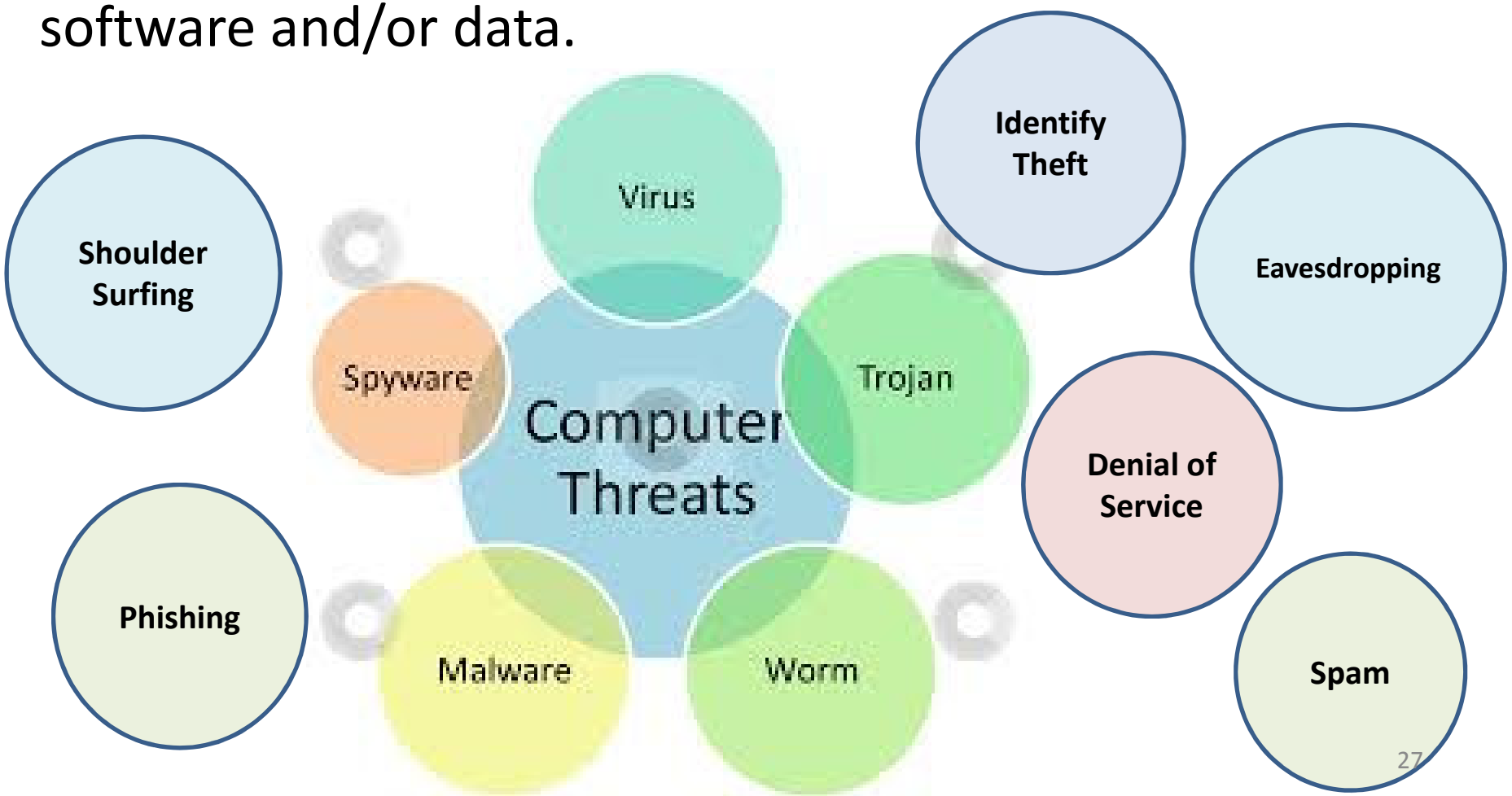
Human Error…accidently deleting information
Equipment Failure
Software Failure
Misrouting/re-routing of messages
Loss or absence of key personnel

Most security breaches originate internally!

- Studies show most security breaches by internal employees are not intentional.
- They happen when employees make bad or uninformed choices about their passwords, the websites they visit, and the e-mails they send.

Intentional Threats

Intentional Threats are those threats that are deliberately designed to harm or manipulate an information system, its software and/or data.



Identify Theft

Identity theft happens when someone steals your personal information and uses it without your permission.

Identity Theft

- Identity theft can make it hard for you to get credit, a job, a place to live, or utilities. But you can reduce your risk of being hurt by identity theft.

- Protect your personal information. That helps you protect your identity.

Identify Theft …Tips to Protect Yourself

- Create secure PIN's and passwords.
- Install security software on all devices.
- Carry only essential documents on person
- Do not give out personal info over the phone.
- Stay on top of your credit and bill/statements.
- Make sure you're in a secure wireless network before connecting to private sites.
- Your trash is their treasure...shred!

Instead of attacking a computer, Social Engineering is the act of interacting and manipulating people to obtain important/sensitive information or perform an act that is latently harmful.

Social Engineering

Posing as Company Employees

A person can go into an agency in a uniform posing as a company employee and say they are there to work on a broken device or network problem.

If they convince the person at the reception desk, they can gain access into the system and "sniff" the network. They can access computers and servers, plant trojan horses, viruses, and create backdoors.

The possibilities are endless.

Other Social Engineering Tactics:

Phishing

Phishing - pretending to be a business to trick you into giving out your personal information.

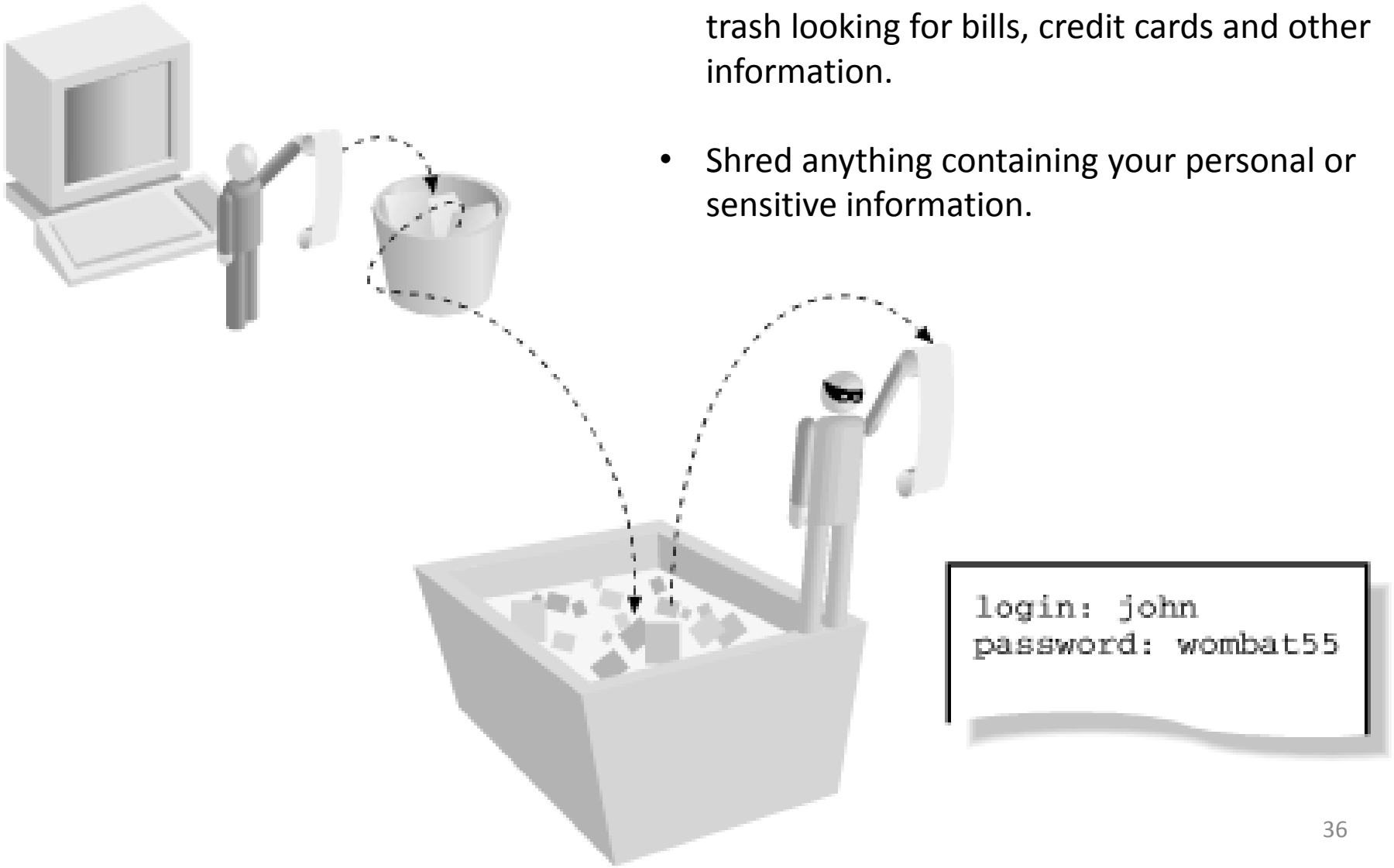
- Thieves can send spam or pop-up messages to get you to reveal your personal information.
- Be sure your firewall, anti-virus, and anti-spyware software is up to date.
- Use identity theft protection.
- Never click on links in pop-up windows or in spam e-mail.

Shoulder Surfing

When a person looks over another person's shoulder and watches keystrokes or views data as it appears on a computer screen.

Dumpster Diving

- Dumpster Diving thieves will go through your trash looking for bills, credit cards and other information.
- Shred anything containing your personal or sensitive information.



- Never allow anyone to follow you into the building or secure area without his or her badge.
- Be aware of procedures for entering a secure area, securing your workstation when you leave the office, and securing your workstation during emergencies.
- Escort visitors to and from your office and around the facility.
- Report any suspicious activity to the security office.
- Do not allow anyone to use personal entry cards/codes for building or secure area access.

Some people will intentionally listen in on others.

Eavesdropping can be an intentional threat. A tactic used by Social Engineering attackers to gather information they are not authorized to have.

Be aware of your surroundings, don’t share information with people who weren’t invited into the conversation.

Malware

Malware is a term that is used for malicious software that is designed to do damage or unwanted actions to a computer system.

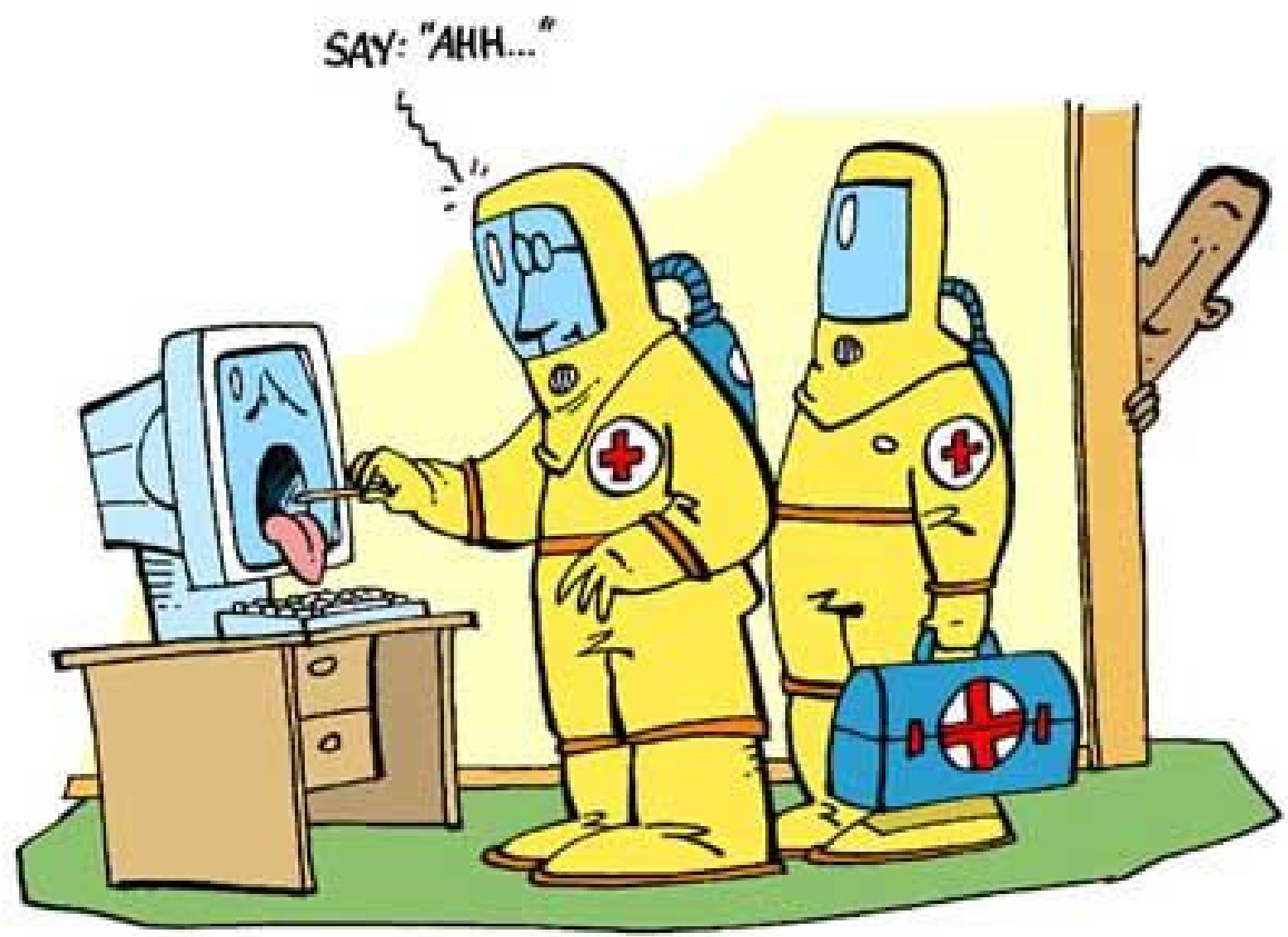
- Viruses
- Worms
- Trojan horses
- Spyware
- Rouge security software

New viruses, worms, and other threats are created by cyber terrorists and discovered **everyday.** If you updated your software yesterday, and a new virus is found today, your software won't protect you….

What is a Computer Virus?

- *Computer viruses* are small malicious software programs designed to spread to multiple computers…infecting your programs and files, altering the way your computer operates or stop it from working altogether.

What Are The Symptoms of Infected Computer???



The Symptoms…

- You see unexpected messages or images…pop ups.
- Programs start unexpectedly.
- Your friends tell you that they have received e-mail messages from your address and you haven't sent them anything.
- Your computer 'freezes' frequently, or programs start running slowly.
- You get lots of system error messages.
- The operating system will not load when you start your computer.
- You notice that files or folders have been deleted or changed.
- Your web browser behaves erratically, e.g. you can't close a browser window.
- Unexpected or excessive activity on hard drive.

How to deal with a Virus Alert:

Did Your Antivirus Say a Virus Was Detected?

- If you saw a message pop up that says a virus was detected, that's a **GOOD** thing. Your antivirus noticed a virus and likely removed it without prompting you.
- In other words, a "virus detected" message that occurs during normal use of your computer doesn't mean your computer was ever infected or that the virus ever did anything.
- If you see a message like this, you're likely visiting an infected web page or downloading a harmful file.
- Remember…Your "real" anti virus will NEVER ask to download anything to fix what it already knows about.

You can also go into your antivirus program and check its quarantine or its virus detection logs to view more information about the virus and what action was taken.

Contact the appropriate personnel. LEAVE the notice on the screen (if possible) for review by an experienced computer technician.

How to remove malware such as a virus, spyware, or rogue security software

Removing a computer virus or spyware can be difficult without the help of malicious software removal tools.

Some computer viruses and other unwanted software reinstall themselves after the viruses and spyware are detected and removed.

Updating the computer and using malicious software removal tools can help remove unwanted software. But nothing can be guaranteed 100% safe.

Incident Response

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies.

Promptly notify the appropriate staff if you become aware of a possible security incident.

SPAM

Definition: The term **spam** refers to unsolicited commercial advertisements distributed online.

Spam is most often considered to be electronic junk mail.

Unknown E-Mail Attachments

Email attachments are a way for a sender to transmit files to another user via email.

These emails can often contain links to malicious web sites or have attachments containing malicious software.

What to do if I opened a malicious attachment?

If you suspect that you have clicked on a malicious attachment:

- Disconnect the computer from the network immediately.

- Scan your computer with **up-to-date** Anti-Virus software.

- Do not input sensitive information into the computer until the Anti-Virus scan has run.

How can I avoid it from happening?

- The best defense against malicious attachments is to keep the Anti-Virus up to date.

- Be suspicious of any email attachments from unknown sources or with offers that seem too good to be true.

- Never open an email attachment you are unsure about.

  As a general rule of thumb you should never click or open an attachment which seems suspicious, in any circumstances, even if it is from someone you know. In other words, don't open attachments unless you are expecting the specific attachment from a known sender.

Keep in mind that a standard Firewall will not:

Stop you from opening e-mail with dangerous attachments.

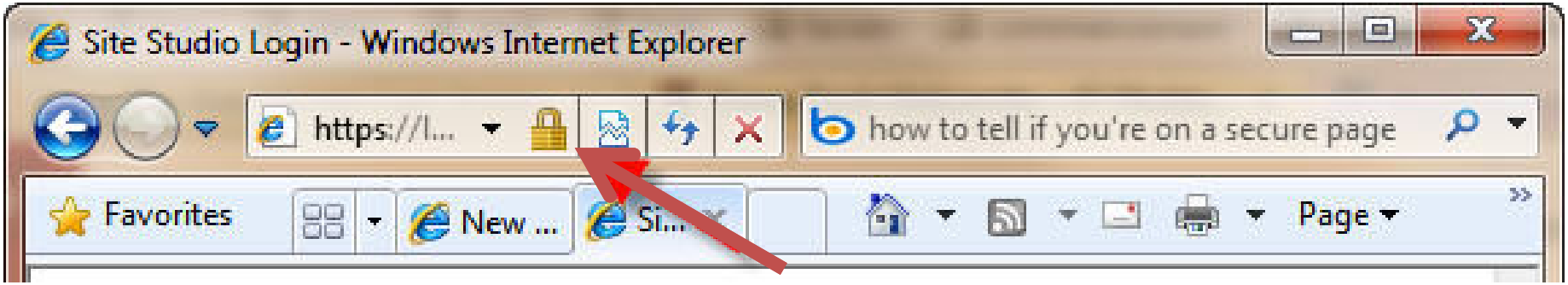
Block spam or unsolicited e-mail from appearing in your inbox.

Detect or disable computer viruses and worms if they are already on your computer.

How to stay safe and secure online

- **Secure your passwords**.
- **Browse smart**

- **URLs that start in "https**" not "http" (It is an encrypted form of information transfer on the internet.)
- **Limit the amount** of personal information you share online.



- **Check the security lock…** To verify a website is genuine, double click on the security lock to display the website's security certificate.
- If the name on the certificate and the address of the website do not match, then the website might be phony.

Internet

Use caution when downloading files from the Internet.

- Make sure that the website is legitimate and reputable. Verify that an anti-virus program has checked the files on the download site.
- Don’t forget…information posted online may be more public than you think!

Antivirus Software

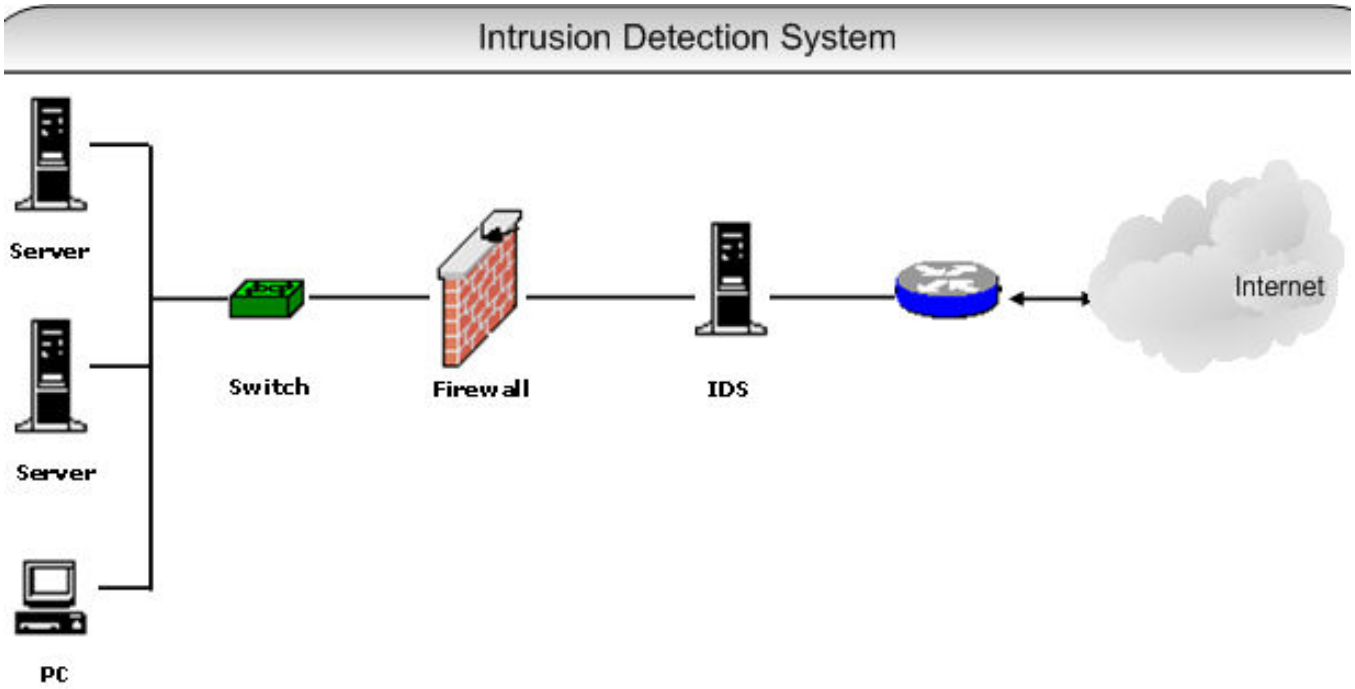
Antivirus software will regularly scan your computer and seek out viruses and other malicious software that might be on your computer.

It is generally recommended that you run auto updates nightly or at least weekly. If you don't know…contact your IT staff.

- There are so many new versions of malware released every day that **no anti-virus program can detect and protect against all of them**.

Intrusion Detection

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.



ENCRYPTION

Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data.

For example, one may wish to encrypt files on a hard disk to prevent an intruder from reading them.

Does your agency have an official written policy on personal equipment…flash drives, cell phones, tablets?

Research shows that BYOD raises security risks.

It’s risky to assume that prohibiting personal devices solves the problem, because many employees end up using their own devices anyway, unmonitored and undeterred by your security policies.

How to secure BYOD

The first and best defense in securing BYODs begins with the same requirements you apply to devices that are already on your network.

These security measures include:

- Enforcing strong passcodes on all devices.
- Antivirus protection and data loss prevention.
- Full-disk encryption for disk, removable media and cloud storage.
- Mobile device management to wipe sensitive data when devices are lost or stolen.
- Application control.

Your agency needs to establish and document the how and when's of allowing personally owned devices to be used.

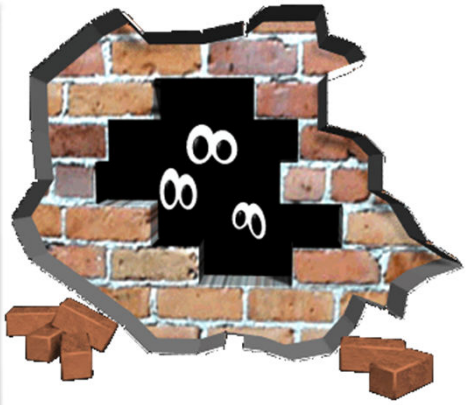
Mobile Risk Mitigations

- Smart phones, laptops, tablet PCs and USB devices… can create new risks to the security of information systems and privacy of protected data.

- How do you ensure that critical information remains secure on personal mobile devices - even when the devices are lost or stolen? Can you do a remote wipe of the device?

Laptop Security

Spyware Protection



Personal Firewall

Laptops and Mobile Devices Added Security

- Disable Bluetooth and wireless when not actively using them.
- Set the device to “ask” before connecting to any unknown wireless networks.
- Remove apps and plug-ins you do not actively use.
- Go through the wireless services list and delete the ones no longer needed.

USB Drives: Could You Be Plugging Malware into Your PC?

Studies show that malware is spread through the use of USB drives. This usually happens when malware from an infected PC is transferred onto a USB drive, without the user ever knowing.

These “dirty” USB then passes along the infection to new computers they encounter.

It does not take long for a large number of computers to be infected. If people are using drives on both shared work and personal computers, it can spread quite rapidly.

USB Device Protection

Protect your data. **Avoid storing sensitive data on Flash Drives**.

But if you must…

- Use encryption.
- Use secure devices. Some of the newer model USB drives have safety features such as fingerprint authentication that protect data from would-be hackers. Others have built-in encryption.
- Store in a safe place…USB drives can be easily lost or misplaced.
- Keep home, office devices separate***.
- Delete all data on the device before you dispose of it.
- Disable Auto run.

***This includes your smartphone…even if you are just charging it.

Device Backups/System Images

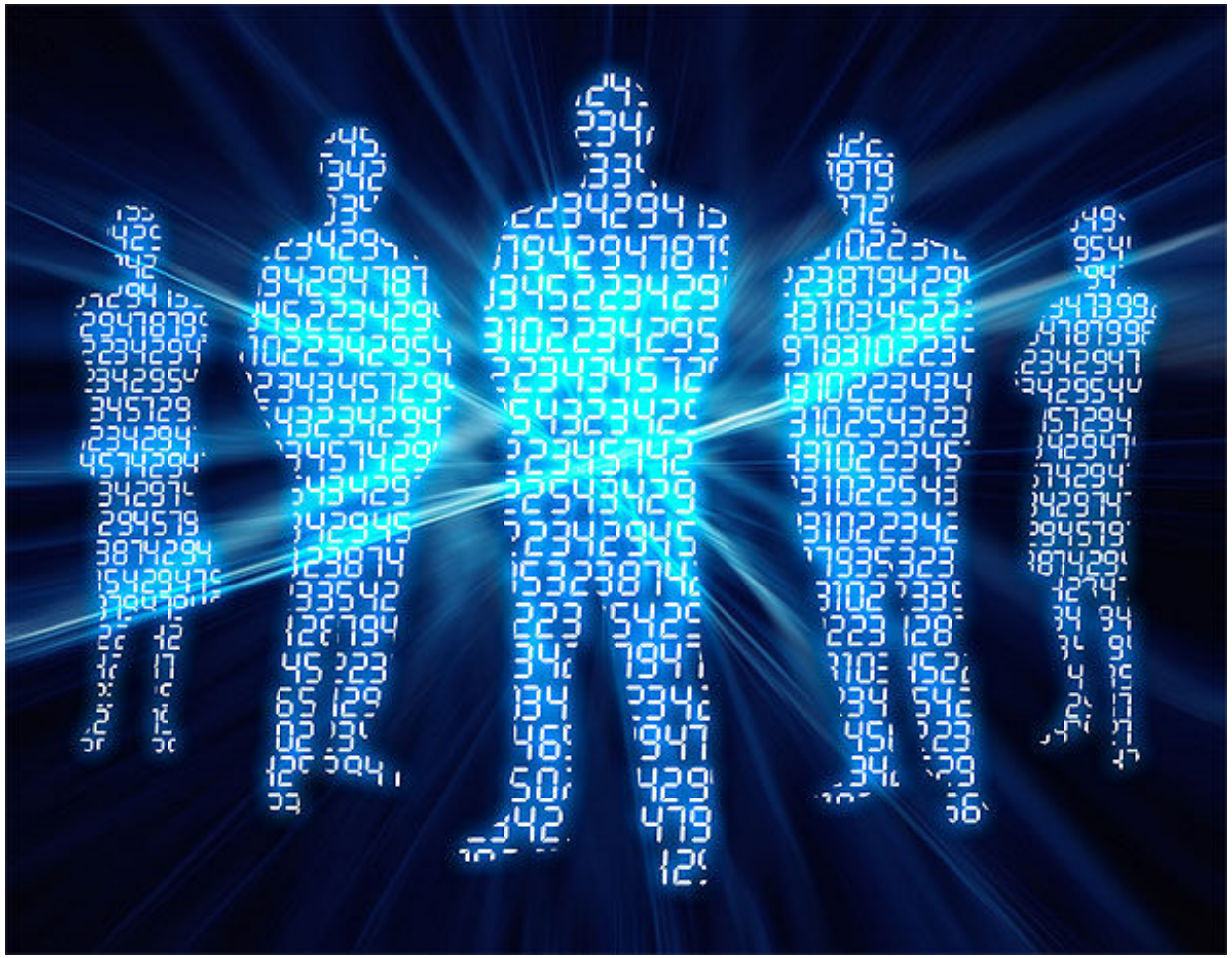
Implement a **backup** and recovery plan. Backing up can protect against hardware failures, important files being deleted, data base corruption, and natural disasters that can leave your office in ruin.

A computer can be restored from a **system image** backup. Reimaging a PC often takes just several minutes, as opposed to the hours of a Windows reinstall.

Device Back up

- Securely store sensitive or critical data.
- Store the back ups away from your computer in case of disaster or theft.
- On occasion, test the restore capability from the backups.
- Don’t forget your mobile devices!!

Personnel with Information Technology Roles



System Patches

A patch is a piece of software that is used to correct a problem with an application operating system or a software program.

Though meant to fix problems, poorly designed patches can sometimes introduce new problems.

Patches should be installed in a test environment (one computer), prior to being installed in a live, operational system.

Access Control (Information Security)

Security features that control who can access resources in the operating system is called *Access Control.*

Various types of users need different levels of access - Internal users, private contractors, outsiders, etc.

Network Infrastructure Protection

- Firewall
- Antivirus
- Robust Passwords
- Encryption
- Physical Security
- Lock Down Your Wi-Fi
- Manage Remote Access
- Secured Wireless

Computer services are programs that listen and respond to network traffic.

Do you know there are many useless services that can slow down a computer? They not only take memory resources but can also be used by spyware.

Examples:

- Open ports
- Remote Access programs (remote desktop)
- Web servers, file servers, proxy and email servers
- All guest accounts should be disabled

If You Don't Need It…Turn It OFF

Helpful Websites

Click on the following links for short Security Awareness Videos and Games

Identity Theft /Video

Malware/ Video

Wireless /Video

Computer Security/Video

Spam/Game

Cyber Criminal/Game

Phishing Scams /Game

Click here to test your PASSWORD STRENGTH!!!

Click mouse to advance to next screen.

You Have Completed Security Awareness Training